(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－190667

(43)公開日　平成９年(1997)７月22日

(51)Int.Cl.⁶	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｇ１１Ｂ　19/02	５０１		Ｇ１１Ｂ　19/02	５０１Ｑ	
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｂ	

審査請求　未請求　請求項の数44　ＯＬ　（全 17 頁）

(21)出願番号　特願平8－985

(22)出願日　平成８年(1996)１月８日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　中村　誠一
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

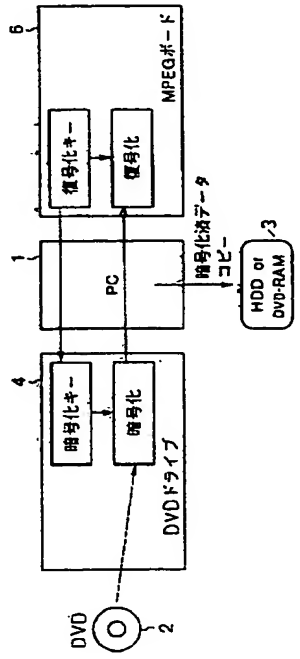
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　複製制御方法及び複製制御装置

(57)【要約】

【課題】本発明は、ドライブから情報伝達手段に受け渡される情報を、情報再生装置で生成したキー情報を用いて暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみがドライブで読出した情報を複製し再生できるようにして、大容量記録媒体、通信媒体等の媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステムが構築できることを特徴とする。

【解決手段】ＭＰＥＧボード６は当該ボードで生成したキー情報をＤＶＤドライブ４に発行する。ＤＶＤドライブ４は上記キー情報をもとにして暗号化キー情報を生成し、当該キー情報によりＤＶＤ２より読出された提供情報を暗号化処理し、ＭＰＥＧボード６に送出する。ＭＰＥＧボード６は当該ボードで生成したキー情報を用いて暗号化処理された提供情報を復号化処理する。



1

【特許請求の範囲】

【請求項１】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置として記録できる手段とを備えたシステムに於いて、

ドライブは、情報再生装置よりキー情報を受け、当該キー情報をもとに大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に渡し、

情報再生装置は、情報伝達手段から受けた暗号化処理された情報をドライブに発行したキー情報に関連するキー情報により復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。

【請求項２】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を記録できる手段とを備えたシステムに於いて、

情報再生装置がドライブにキー情報を発行し、

ドライブが情報再生装置より受けたキー情報をもとに大容量記録媒体より読出した情報を暗号化処理し情報伝達手段に渡して、

ドライブにキー情報を発行した情報再生装置のみが情報伝達手段を介して記録した情報を復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。

【請求項３】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブと情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成し、

ドライブが、自己生成した一時的なキー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した一時的なキー情報を用いて情報伝達手段より受けた情報を復号化して、

ドライブより読出した情報の再生を可能にし、ドライブより読出した情報を一旦記録した複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

【請求項４】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

少なくともドライブ又は情報再生装置が、ランダムな情報をもとに一次キー情報を生成し、当該キー情報をもとにしてドライブ及び情報再生装置がそれぞれ一時的な二次キー情報を自己生成し、

ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、

ドライブより読出された情報の再生を可能にし、複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

2

【請求項５】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブ及び情報再生装置のそれぞれが、ランダムな情報をもとに一次キー情報を生成し、当該キー情報を相互に受け渡し、その各一次キー情報をもとにして一時的な二次キー情報を自己生成し、

ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、

暗号化及び復号化に供されるキー情報を情報伝達手段から隠して、複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

【請求項６】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブは、大容量記録媒体より、再生の対象となる情報の読出しに際して、特定の制御情報を読み、その制御情報から、当該記録媒体より読出され一旦記録された複製情報に対しての複製許可レベルを認識して、

複製許可レベルが特定の情報再生装置でのみ複製情報の再生を許可するレベルであるとき、再生を行なう情報再生装置よりキーのもとになる情報を受け、当該情報をもとに生成したキー情報により、大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に受け渡し、

複製許可レベルが全ての情報再生装置での複製情報の再生を禁止するレベルであるとき、再生を行なう情報再生装置よりランダムな情報を受け、当該情報をもとに一時的なキー情報を生成して、当該キー情報により大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に受け渡して、

大容量記録媒体に記録した特定の制御情報により、複製情報の複製許可を任意にコントロールできるようにしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

【請求項７】　情報伝達手段は、コンピュータ装置又は情報伝送装置又は伝送する情報の記録が可能な他の装置により実現される請求項１又は２又は３又は４又は５又は６記載の複製制御方法。

【請求項８】　情報再生装置は、ＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４を対象としたＭＰＥＧデコーダを搭載した再生ボードにより実現される請求項１又は２又は３又は４又は５又は６記載の複製制御方法。

【請求項９】　大容量記録媒体は、ＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４で圧縮された映像情報を含む提供情報を固定記録したディスクにより実現される請求項１又は２又は３又は４又は５又は６記載の複製制御方法。

【請求項１０】　情報再生装置で生成したキー情報を複製情報に対応付けて保存する手段をもつ請求項１又は２又は３記載の複製制御方法。

【請求項１１】　任意の値をもつキー情報を設定できる請求項１又は２又は３記載の複製制御方法。

【請求項１２】　少なくとも暗号化又は復号化の処理に用いられるキー情報は、少なくとも再生の開始又は終了の都度、内容が変更される１又は２又は３又は４又は５又は６記載の複製制御方法。

【請求項１３】　情報再生装置は、互いに関連付けされた暗号化のキー情報及び復号化のキー情報をもち、少なくとも暗号化のキー情報を暗号化処理してドライブに送出する手段をもつ請求項１又は２記載の複製制御方法。

【請求項１４】　大容量記録媒体より読出される特定の制御情報の内容が変る度に、少なくとも暗号化又は復号化の処理に用いられるキー情報の内容が変更される請求項６記載の複製制御方法。

【請求項１５】　ドライブと情報再生装置との間で受け渡されるキー情報が情報伝達手段上に於いて暗号化処理される請求項１又は３又は４又は５又は６記載の複製制御方法。

【請求項１６】　大容量記録媒体に記録されドライブ装置で読出された情報を受けて再生処理するデコーダを備えた情報再生装置に於いて、ドライブより受けた情報を復号化するためのキー情報を内部に発行し、ドライブより出力される情報を暗号化するためのキー情報をドライブに発行する手段を設けてなることを特徴とした大容量記録媒体の情報再生装置。

【請求項１７】　大容量記録媒体に記録された情報を読出して情報再生装置に受け渡す大容量記録媒体のドライブ装置に於いて、大容量記録媒体に記録された情報を再生する際に情報再生装置よりキー情報を受けて保持する手段と、このキー情報をもとにして情報再生装置へ転送する情報を暗号化する手段とを具備してなることを特徴とする大容量記録媒体のドライブ装置。

【請求項１８】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステムに於いて、

情報再生装置に、キー情報の生成手段、及びキー情報をドライブに発行する手段を設け、

ドライブに、上記キー情報を受け、このキー情報をもとに大容量記録媒体から読出した情報を暗号化処理する手段を設けて、

ドライブにキー情報を発行した情報再生装置のみが複製情報を再生できることを特徴とする複製制御装置。

【請求項１９】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブ及び情報再生装置に、互いに関連する情報で個別にキー情報を生成する手段を設け、

ドライブに、自己生成したキー情報を用いて、情報伝達手段に出力する情報を暗号化する手段を設け、

情報再生装置に、自己生成したキー情報を用いて、情報伝達手段より受けた情報を復号化する手段を設けて、

暗号化及び復号化に用いるキー情報を情報伝達手段より隠したことを特徴とする大容量記録媒体に記録された情報の複製制御装置。

【請求項２０】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

少なくともドライブ又は情報再生装置に、ランダムな情報をもとに一次キー情報を生成する手段を設け、

ドライブ及び情報再生装置に、上記一次キー情報をもとにして一時的な二次キー情報を自己生成する手段を設けて、

ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することを特徴とした複製制御装置。

【請求項２１】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブ及び情報再生装置のそれぞれに、ランダムな情報をもとに一次キー情報を生成する手段と、その双方で生成された各一次キー情報を用いて二次キー情報を生成する手段とを設け、

ドライブが自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することを特徴とする複製制御装置。

【請求項２２】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステムに於いて、

ドライブ及び情報再生装置に、相互に関連するキー情報を保持する手段と、大容量記録媒体に記録された特定の制御情報を受けて、大容量記録媒体から読出される情報の複製許可レベルを判断する手段とを設け、

ドライブに、複製許可レベルに応じて、大容量記録媒体より読出した情報を、関連するキー情報をもつ情報再生

装置でのみ複製情報を復号処理できるように暗号化処理し、又は全ての情報再生装置が複製情報を復号処理できないように暗号化処理し、又は暗号化処理を施さずに情報伝達手段に受け渡す手段とを設けて、
大容量記録媒体に記録された特定の制御情報により、複製情報の複製許可を任意にコントロールできるようにしたことを特徴とする複製制御装置。

【請求項２３】　情報再生装置に、キー情報の生成手段、及びキー情報をドライブに発行する手段を設け、ドライブに、上記キー情報を受け、このキー情報をもとに大容量記録媒体から読出した情報を暗号化処理する手段を設けて、複製情報の再生を特定の情報再生装置でのみ可能とした請求項２２記載の複製制御装置。

【請求項２４】　ドライブ及び情報再生装置に、互いに関連する情報で個別にキー情報を生成する手段を設け、ドライブに、自己生成したキー情報を用いて、情報伝達手段に出力する情報を暗号化する手段を設け、情報再生装置に、自己生成したキー情報を用いて、情報伝達手段より受けた情報を復号化する手段を設けて、全ての情報再生装置が複製情報を復号処理できないようにした請求項２２記載の複製制御装置。

【請求項２５】　情報伝達手段は、コンピュータ装置又は情報伝送装置又は伝送する情報の記録が可能な他の装置により実現される請求項１８又は１９又は２０又は２１又は２２又は２３記載の複製制御装置。

【請求項２６】　情報再生装置は、ＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４を対象としたＭＰＥＧデコーダを搭載したボードにより実現される請求項１８又は１９又は２０又は２１又は２２又は２３記載の複製制御装置。

【請求項２７】　大容量記録媒体はＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４で圧縮された映像情報を含む提供情報を固定記録したディスクにより実現される請求項１８又は１９又は２０又は２１又は２２又は２３又は２４記載の複製制御装置。

【請求項２８】　情報再生装置で生成したキー情報を複製情報に対応付けて保存する手段をもつ請求項１８又は２２又は２３記載の複製制御装置。

【請求項２９】　任意の値をもつキー情報を設定できる請求項１８又は２２又は２３記載の複製制御装置。

【請求項３０】　少なくとも暗号化又は復号化の処理に用いられるキー情報は、少なくとも再生の開始又は終了の都度、内容が変更される請求項１８又は１９又は２０又は２１又は２２又は２３又は２４記載の複製制御装置。

【請求項３１】　情報再生装置は、互いに関連付けされた暗号化のキー情報及び復号化のキー情報をもち、少なくとも暗号化のキー情報を暗号化処理してドライブに送出する手段をもつ請求項１８又は２２記載の複製制御装置。

【請求項３２】　大容量記録媒体より読出される特定の

制御情報の内容が変る度に、少なくとも暗号化又は復号化の処理に用いられるキー情報の内容が変更される請求項２２又は２３又は２４記載の複製制御装置。

【請求項３３】　ドライブと情報再生装置との間で受け渡されるキー情報が情報伝達手段上に於いて暗号化処理される請求項１８又は２０又は２１又は２２記載の複製制御装置。

【請求項３４】　通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えてなるシステムに於いて、
情報再生装置が情報提供装置にキー情報を発行し、情報提供装置が情報再生装置より受けたキー情報をもとに提供先の情報再生装置に送信する情報を暗号化処理して、暗号化処理に用いられたキー情報を発行した情報再生装置のみが複製情報を再生できることを特徴とする通信により提供される情報の複製制御方法。

【請求項３５】　通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、
情報提供装置と情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成し、情報提供装置が自己生成した一時的なキー情報を用いて通信手段に送出する情報を暗号化し、情報再生装置が自己生成した一時的なキー情報を用いて通信手段を介して受けた情報を復号化して、
通信手段を介して受けた情報の再生を可能にし、当該情報を一旦記録した複製情報の再生を不可にしたことを特徴とする通信により提供される情報の複製制御方法。

【請求項３６】　通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、
情報提供装置は、複製情報の許可レベルを指定する複製許可情報を情報再生装置に送出し、
情報再生装置は、情報提供装置より受けた複製許可情報をもとに、提供される情報の複製の許可レベルを認識して、
複製情報の再生が可能な許可レベルであるときは、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡し、
複製情報の再生が特定の情報再生装置でのみ可能な許可レベルであるときは、情報再生装置よりキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡し、
複製情報の再生を禁止する許可レベルであるときは、情

報提供装置及び情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成し、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡すことを特徴とする通信により提供される情報の複製制御方法。

【請求項３７】　通信手段は、コンピュータ装置と当該装置に接続される通信回線とにより実現される請求項３４又は３５又は３６記載の通信により提供される情報の複製制御方法。

【請求項３８】　通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、

情報再生装置に、当該装置に固有のキー情報を生成する手段を設け、

情報提供装置に、情報再生装置よりキー情報を受け、当該キー情報をもとに提供情報を暗号化処理する手段を設けて、

暗号化処理に供されたキー情報をもつ情報再生装置のみが複製情報を再生できることを特徴とする通信により提供される情報の複製制御装置。

【請求項３９】　通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、

情報提供装置及び情報再生装置のそれぞれに、互いに関連する情報で個別にキー情報を生成する手段する手段を設け、

情報提供装置が自己生成したキー情報を用いて通信手段に送出する提供情報を暗号化処理し、情報再生装置が自己生成した情報を用いて通信手段を介して受けた情報を復号化することを特徴とする通信により提供される情報の複製制御装置。

【請求項４０】　通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、

情報提供装置に、情報提供に際して当該情報の複製許可レベルを認識する手段と、複製許可情報が複製情報の再生を許可するレベルであるとき、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡す手段と、

複製許可情報が、複製情報の再生を特定の情報再生装置のみ許可するレベルであるとき、再生を行なう情報再生装置が生成したキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介して情報再生装置に受け渡し、

複製許可情報が、複製情報の再生を許可しないレベルであるときは、再生を行なう情報再生装置よりランダムな情報を受け、当該情報をもとに一時的なキー情報を生成して、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介して情報再生装置に受け渡すことを特徴とする通信により提供される情報の複製制御装置。

【請求項４１】　通信手段は、通信回線、及び当該回線に回線接続されたコンピュータ装置により実現される請求項３８又は３９又は４０記載の通信により提供される情報の複製制御装置。

【請求項４２】　情報再生装置はＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４を対象としたＭＰＥＧデコーダを搭載したボードにより実現される請求項３８又は３９又は４０又は４１記載の通信により提供される情報の複製制御装置。

【請求項４３】　情報提供装置はＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４で圧縮された映像情報を含む提供情報を通信手段を介し情報再生装置に送信する請求項３８又は３９又は４０記載の通信により提供される情報の複製制御装置。

【請求項４４】　映像情報を含む提供情報を記録した媒体から情報を読出す読出装置と、この読出装置に接続されるコンピュータ装置と、このコンピュータ装置で受取った提供情報を再生処理するボードと、コンピュータ装置に渡された情報を複製情報として記録できる手段とを備えたコンピュータシステムであって、

読出装置には、乱数により任意の第１のキー情報を発生する手段と、第１のキー情報を保持する手段と、ボードより第２のキー情報を受けて保持する手段と、第１のキー情報と第２のキー情報から第３のキー情報を生成する手段と、ボードよりボードに固有の暗号化された第５のキー情報を受け第３のキー情報により復号化して保持する手段と、第１のキー情報をボードに送出する手段と、媒体から複製許可情報を読出し保持する手段と、複製許可情報に従い第３のキー情報又は第５のキー情報を用いて媒体から読出した提供情報を選択的に暗号化処理する手段とを具備し、

ボードには、乱数により任意の第２のキー情報を発生する手段と、第２のキー情報を保持する手段と、第２のキー情報を読出装置に送出する手段と、読出装置より第１のキー情報を受けて保持する手段と、第１のキー情報と第２のキー情報から第４のキー情報を生成する手段と、ボードに固有の第５，第６のキー情報を発生する手段と、第５のキー情報を第４のキー情報を用いて暗号化し読出装置に送出する手段と、読出装置から複製許可情報を受けて保持する手段と、複製許可情報に従い第４のキー情報又は第６のキー情報を用いてコンピュータ装置より受けた提供情報を選択的に復号化処理する手段とを具備して、

第５のキー情報を用いて暗号化処理し、第６のキー情報

を用いて復号化処理したとき、当該各キー情報を発行したボードのみが、媒体より読出した情報の複製情報を再生可能にし、

第3のキー情報を用いて暗号化処理し、第4のキー情報を用いて復号化処理したとき、媒体より読出した情報の再生を可能にし、複製情報の再生を不可にすることを特徴とした複製制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばMPEG2等により圧縮処理された映画、音楽等の情報（提供情報と称す）を再生出力する提供情報の再生機能をもつ情報処理システムに適用される複製制御方法及び複製制御装置に関する。

【0002】本発明は、例えばCD－ROM、DVD（ディジタルビデオディスク）等の大容量記録媒体に記録された情報を複製情報として記録し再生する際の複製情報の再生利用を当該媒体に記録された特定の制御情報によりコントロールできる複製制御方法及び複製制御装置に関する。

【0003】本発明は、通信手段を介して映画、音楽等の提供情報を受信し、当該提供情報を再生出力する機能を備えたコンピュータシステムに適用される、通信により提供される情報の複製制御方法及び複製制御装置に関する。

【0004】

【従来の技術】映画産業や音楽産業から提供される、例えばMPEG2等により圧縮処理された、映画、音楽等の情報（提供情報と称す）を再生出力するシステムに於いては、不正な複製を防止するためのコピープロテクト技術が必要とされる。

【0005】特に、上記したような付加価値の高い提供情報をコンピュータ処理して再生出力するシステムに於いては、コンピュータ処理で解除されてしまう程度のコピープロテクト技術ではなく、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術の確立が必要不可欠とされる。

【0006】従来のこの種コピープロテクト技術は、提供情報を記録したCD－ROM等の記録媒体に、不正複製防止情報を併せて記録しておき、この不正複製防止情報を提供情報とともに読出して不正複製防止装置に伝送し、提供情報に複製防止の加工を施すことにより不正複製を防止している。

【0007】しかしながら、このような従来のコピープロテクト技術に於いては、ディスクに記録されている提供情報が不正複製防止装置に伝送されるまで複製防止の加工が施されておらず、従ってディスクの読出装置と再生装置との間に伝送装置としてコンピュータ装置が介在するようなシステム構成に於いては提供情報の故意の不正複製を許してしまう。

【0008】このように、従来では、提供情報の受け渡しにコンピュータが介在するシステムに於いて、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術が確立されておらず、特に、提供情報の一部を選択的にコンピュータに取り込んで利用できるシステムを構築しようとしたとき、全ての提供情報を対象に不正な複製を許してしまうという問題があった。

【0009】

【発明が解決しようとする課題】上述したように、従来では、大容量記録媒体等により提供される映画情報、音楽情報等の提供情報の受け渡しにコンピュータが介在するシステムに於いて、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術が確立されておらず、特に、提供情報の一部を選択的にコンピュータに取り込んで利用できるシステムを構築しようとしたとき、全ての提供情報を対象に不正な複製を許してしまうという問題があった。

【0010】本発明は上記実情に鑑みなされたもので、大容量記録媒体等により提供される情報の受け渡しにコンピュータが介在するシステムに於いても、不正な複製を確実に防止することのできる信頼性の高い複製制御方法及び複製制御装置を提供することを目的とする。

【0011】又、本発明に於いては、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ装置が介在するシステムに於いても、コンピュータ装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能な複製制御方法及び複製制御装置を提供することを目的とする。

【0012】

【課題を解決するための手段】本発明は、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いて、コンピュータ等の複製処理が可能な装置上では、媒体より読出された情報が特定のキーにより暗号化された状態であるため、複製情報の再生可否を任意にコントロールできる。

【0013】又、本発明は、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いて、コンピュータ等の複製処理が可能な装置に、暗号化及び復号化の処理に用いるキー情報を直接見せずに、媒体側で提供情報毎に複製情報の再生利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製の再生による提供情報の活用が可能な複製制御方法及び複製制御装置を提供する。尚、本発明に於いては、大容量記録媒体、通信媒体等により提供される情報を記憶装置等に一旦記録し、読出して再生することを「複製情報の再生」と称している。

【００１４】即ち、本発明は、大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステムに於いて、ドライブから情報伝達手段に受け渡される情報を、情報再生装置で生成したキー情報を用いて暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみが複製情報を再生できる（即ち一世代コピーを許可する）ことを特徴とする。

【００１５】又、上記システムに於いて、ドライブ及び情報再生装置のそれぞれが、ランダムな情報をもとに互いに関連するキー情報を個別に生成し、ドライブが、自己生成したキー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、暗号処理及び復号処理に用いたキー情報を情報伝達手段に渡すことなく、関連するキー情報をもつ情報再生装置のみの再生を許可し、複製情報の再生を不可にすることを特徴とする。

【００１６】又、上記システムに於いて、ドライブ及び情報再生装置が、大容量記録媒体に記録された特定の制御情報をもとに、複製許可レベルを認識し、複製情報の再生を許可するレベルであるときは、ドライブより読出した情報を暗号化処理せずに情報伝達手段に受け渡し、複製情報の再生を特定の情報再生装置でのみ許可するレベルであるときは、ドライブより読出した情報を、再生を行なう情報再生装置で生成したキー情報を用いてドライブより読出した情報を暗号化処理した後、情報伝達手段に受け渡し、複製情報の再生を禁止するレベルであるときは、ドライブと情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成して、関連するキー情報をもつ情報再生装置のみドライブより読出した情報の再生を可能にし、関連するキー情報をもつ情報再生装置を含む全ての情報再生装置の複製情報の再生を不可にしたことを特徴とする。

【００１７】又、本発明は、通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、情報提供装置が情報再生装置よりキー情報を受け、当該キー情報をもとにして情報再生装置に提供する情報を暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみが複製情報を再生できることを特徴とする。

【００１８】又、上記システムに於いて、情報提供装置及び情報再生装置のそれぞれが、ランダムな情報をもとに互いに関連するキー情報を個別に生成し、情報提供装置が自己生成した暗号化キー情報を用いて情報再生装置に提供する情報を暗号化し、情報再生装置が自己生成した復号化キー情報を用いて情報提供装置より受けた情報を復号化することにより、通信手段を介して受けた情報の再生を可能にし、複製情報の再生を不可にしたことを特徴とする。

【００１９】又、上記システムに於いて、情報提供装置は、複製情報の許可レベルを指定する複製許可情報を情報再生装置に送出し、情報再生装置は、情報提供装置より受けた複製許可情報をもとに、提供される情報の複製の許可レベルを認識して、複製情報の再生が可能な許可レベルであるときは、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡し、複製情報の再生が特定の情報再生装置でのみ可能な許可レベルであるときは、情報再生装置よりキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡し、複製情報の再生を禁止する許可レベルであるときは、情報提供装置及び情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成し、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡すことを特徴とする。

【００２０】上記したような複製制御機構をもつことにより、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いても、コンピュータ等の複製処理が可能な装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製情報の再生を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステムが構築できる。

【００２１】

【発明の実施の形態】以下図面を参照して本発明の実施形態を説明する。図１は本発明の第１の実施形態に於ける基本的なシステム構成を示すブロック図であり、ここでは、大容量記憶媒体（ＤＶＤ２）に記録された、映画、音楽等の提供情報を複製防止の対象として、ドライブ（ＤＶＤドライブ４）から情報伝達手段（ＰＣ１）に受け渡される提供情報を、情報再生装置（ＭＰＥＧボード６）内で生成したキー情報を用いて暗号化処理することで、暗号化処理したキー情報をもつ情報再生装置（ＭＰＥＧボード６）のみがドライブ（ＤＶＤドライブ４）で読出した情報を複製し再生できる、一世代コピーを許可する実施形態を例示している。

【００２２】図１に於いて、１はドライブで読取った提供情報を情報再生装置に受け渡す情報伝達手段となるコンピュータ装置（ＰＣ）であり、ここではドライブで読取った複製許可された提供情報を選択的に取り込み、ＨＤＤ、ＤＶＤ－ＲＡＭ等の外部記憶装置３に記憶して、編集、校正等の処理を可能とする。

【００２３】２は複製制御の対象となる映画、音楽等の提供情報を記録したＤＶＤディスクである。このＤＶＤ

２には、上記提供情報が例えばＭＰＥＧ２により圧縮処理して記録されるとともに、この提供情報に対応して、メディア・ファイル管理情報ブロックの一部に、図７に示すような複製許可情報（ＣＧＭＳ）が記録される。

【００２４】４はＤＶＤ２の情報を読取るドライブ装置であり、ここではＤＶＤドライブと称している。このＤＶＤドライブ４は、情報再生装置内で生成したキー情報を受け、当該キー情報を用いて、ＤＶＤ２より読取った提供情報を暗号化処理する機能をもつ。この機能の具体的な構成例は図２に示される。

【００２５】６はＤＶＤドライブ４で読取った提供情報をコンピュータ装置（ＰＣ）１を介して受け再生出力処理する情報再生装置であり、ここではＭＰＥＧボードと称している。このＭＰＥＧボード６は、ＭＰＥＧ２デコーダを搭載し、コンピュータ装置（ＰＣ）１を介して受けた、ＭＰＥＧ２により圧縮処理された提供情報をデコードして再生出力情報を得る。更にこのＭＰＥＧボード６には、キー情報を生成し、そのキー情報をＤＶＤドライブ４に送出するとともに、そのキー情報を用いて提供情報を復号化処理する機能をもつ。この機能の具体的な構成例は図２に示される。

【００２６】上記図１の構成に於いて、ＭＰＥＧボード６は当該ボード６で生成したキー情報をＤＶＤドライブ４に発行するとともに、当該キー情報を復号化キーとして保持する。

【００２７】ＤＶＤドライブ４は上記キー情報を用いて暗号化キーを生成し、当該キーを用いて、ＤＶＤ２より読出された提供情報を暗号化処理した後、コンピュータ装置（ＰＣ）１を介しＭＰＥＧボード６に送出する。

【００２８】ＭＰＥＧボード６はＤＶＤドライブ４より暗号化された提供情報をコンピュータ装置（ＰＣ）１を介して受け、当該ボードで生成した復号化キーを用いて復号化処理する。

【００２９】このような複製制御機構を備えることにより、暗号化処理に用いたキー情報をもつＭＰＥＧボード６のみがＤＶＤドライブ４で読出した情報を複製情報として記録して再生できる。

【００３０】即ち、ＤＶＤドライブ４が、１種類（又は一つ）の提供情報に対して、１種類の暗号化を施せば、情報伝送装置を介して複数の情報再生装置が接続されていても、暗号化に供されたキー情報をもつ情報再生装置以外は複製情報の再生利用が不可能となる。

【００３１】尚、具体的な構成では、ＭＰＥＧボード６からＤＶＤドライブ４に送られるキー情報には暗号化処理が施される。又、具体的な構成では、上記実施形態による複製の排他制御が上記複製許可情報（ＣＧＭＳ）により選択的に有効となるもので、具体例を挙げると、図７に於いて、ＣＧＭＳのｂ０，ｂ１が“０１”であるとき、上記した複製の排他制御が可能となる。

【００３２】図２は本発明の第２の実施形態に於けるシステム構成を示すブロック図であり、ここでは、大容量記録媒体に記録された複製許可情報（C-GMS）に従い、ドライブより読出された提供情報を一旦記録した複製情報の再生をすべての情報再生装置に対して可能にするコピーフリーの複製許可レベルと、上記複製情報の再生を特定の情報再生装置でのみ可能にする許可レベルと、上記複製情報の再生をすべての情報再生装置に対して許可しない許可レベルとを選択的に切り替える機能ををもつシステムを実現している。

【００３３】図２に於いて、１０及び１０Ａは図１に示すコンピュータ装置（ＰＣ）１に相当するもので、１０はシステム全体の制御を司るコンピュータ本体のＣＰＵ、１０Ａは同システムバスである。ここではＣＰＵ１０の制御の下に、図３乃至図６に示すような複製制御処理が実行される。又、ＣＰＵ１０は、ドライブ装置４０が情報記録媒体２０より読取った複製許可された提供情報を選択的に取り込み、記憶装置３０に記憶して、編集、校正等の処理を可能とする。

【００３４】２０は図１に示すＤＶＤ２に相当する情報記録媒体であり、ここではＭＰＥＧ２により圧縮処理して記録されるとともに、この提供情報に対応して、メディア・ファイル管理情報ブロックの一部に、図７に示すような複製許可情報（ＣＧＭＳ）が記録される。

【００３５】３０は図１に示す外部記憶装置３に相当する記憶装置であり、ここでは複製情報の保存、編集、校正等に供される。４０は図１に示すＤＶＤドライブ４に相当するドライブ装置であり、情報記録媒体２０の情報を読取る。ここでは、暗号生成装置４１，４４、暗号キーを貯えるレジスタ４２，４３，４５，４８、５１、読出装置４６、暗号化装置４７，４９、復号化装置５０等を備えて構成される。

【００３６】暗号生成装置４１は、乱数発生装置を用いたランダムな値をもとに暗号キー（１）を発生する。レジスタ４２は暗号発生装置４１が発生した暗号キー（１）を保持する。レジスタ４３はシステムバス１０Ａを介して再生装置６０より受けた暗号キー（２）を保持する。

【００３７】暗号生成装置４４は暗号キー（１）と暗号キー（２）とを用いて暗号キー（３）を生成する。レジスタ４５は暗号発生装置４４が発生した暗号キー（３）を保持する。

【００３８】読出装置４６は情報記録媒体２０に記録された情報を読出す。ここでは複製制御の対象となる映画、音楽等の提供情報、及び当該提供情報の複製許可レベルを示す図７に示すような複製許可情報（C-GMS）それぞれを読出す。

【００３９】暗号化装置４７は、情報記録媒体２０より読出した提供情報を複製許可情報（C-GMS）に従い、レジスタ４５に貯えられた暗号キー（３）、又はレジスタ５１に貯えられた提供情報暗号化キー（５）を用いて

15

暗号化処理し、又は暗号化処理を施さずに、システムバス１０Ａを介して再生装置６０に送出する。

【００４０】レジスタ４８は情報記録媒体２０より読み取った複製許可情報（ＣＧＭＳ）を保持する。暗号化装置４９はレジスタ４８に貯えられた複製許可情報（ＣＧＭＳ）を暗号化処理してシステムバス１０Ａを介し再生装置６０に送出する。

【００４１】復号化装置５０は再生装置６０より受けた、暗号化処理された装置固有の提供情報暗号化キー（５）を復号化する。レジスタ５１は復号化装置５０で復号化処理された暗号化キー（５）を保持する。

【００４２】６０は図１に示すＭＰＥＧボード６に相当する提供情報の再生装置であり、ＭＰＥＧデコーダを搭載し、システムバス１０Ａを介して受けた、ＭＰＥＧ２により圧縮処理された提供情報をデコードして再生出力情報を得る。ここでは、暗号生成装置６１，６４、暗号キーを貯えるレジスタ６２，６３，６５，６９、７１，７２，復号化装置６６，６７、ＭＰＥＧ２デコーダ６８、暗号化装置７０等を備えて構成される。

【００４３】暗号生成装置６１は、乱数発生装置を用いたランダムな値をもとに暗号キー（２）を発生する。レジスタ６２はシステムバス１０Ａを介してドライブ装置４０より受けた暗号キー（１）を保持する。レジスタ６３は暗号生成装置６１で発生した暗号キー（２）を保持する。

【００４４】暗号生成装置６４は暗号キー（１）と暗号キー（２）とを用いて暗号キー（４）を生成する。レジスタ６５は暗号発生装置６４が発生した暗号キー（４）を保持する。

【００４５】復号化装置６６は、コンピュータ本体のシステムバス１０Ａを介してドライブ装置４０より受けた、暗号化処理された複製許可情報（ＣＧＭＳ）を復号化する。

【００４６】復号化装置６７はコンピュータ本体のシステムバス１０Ａを介してドライブ装置４０より受けた提供情報を、レジスタ７１に貯えられた複製許可情報（ＣＧＭＳ）に従い、レジスタ６５に貯えられた暗号キー（４）、又はレジスタ７２に貯えられた提供情報復号化キー（６）を用いて復号化処理し、又は復号化処理を施さずに、ＭＰＥＧ２デコーダ６８に送出する。

【００４７】ＭＰＥＧ２デコーダ６８は、復号化装置６７で復号化した提供情報をデコード処理して再生出力可能な提供情報を表示コントローラ８０に送出する。レジスタ６９は装置固有の提供情報暗号化キー（５）を保持する。暗号化装置７０はレジスタ６９に貯えられた装置固有の提供情報暗号化キー（５）を暗号化処理してドライブ装置４０に送出する。

【００４８】レジスタ７１は復号化装置６６で復号化された複製許可情報（ＣＧＭＳ）を保持する。レジスタ７２はレジスタ６９に貯えられた装置固有の提供情報暗号

16

化キー（５）と対をなす（例えば値が共通する）提供情報復号化キー（６）を保持する。

【００４９】８０はＭＰＥＧ２デコーダ６８より出力された提供情報を表示装置８１に表示出力する表示コントローラである。尚、レジスタ４５，６５のキー値は、少なくとも再生の開始時又は終了時に一旦クリアされて書き替えられる。又、レジスタ６９，７２のキー値も、固定値のみでなく、例えば、再生の開始時等に書き替える構成であってもよい。

【００５０】図３乃至図６はそれぞれ本発明の第２実施形態に於ける処理手順を示すフローチャートであり、このうち、図３及び図４はそれぞれ暗号化及び復号化処理のための各種キー情報の設定処理手順を示すフローチャート、図５及び図６はそれぞれ提供情報読出し時に於ける複製制御処理手順を示すフローチャートである。

【００５１】図７は情報記録媒体２０に記録されたメディア・ファイル管理情報ブロック内の複製許可情報（ＣＧＭＳ）を説明するための情報フォーマットを示す図である。ここでは、ＣＧＭＳのｂ０，ｂ１が“００”であるとき、全ての再生装置６０に対して複製情報の再生を許可し、ｂ０，ｂ１が“０１”であるとき、提供情報読出し時に利用された再生装置のみに対して排他的な複製情報の再生を許可し、ｂ０，ｂ１が“１１”であるとき、全ての再生装置６０に対して複製情報の再生を不許可にする。

【００５２】ここで図２乃至図７を参照して本発明の第２実施形態に於ける動作を説明する。先ず、図３及び図４に示すフローチャートを参照して、暗号化及び復号化処理のための各種キー情報の設定処理を説明する。

【００５３】再生指示に従うシステム起動に伴い、ドライブ装置４０の暗号発生装置４１はランダムな値をもとに暗号キー（１）を発生する（図３ステップ４０ａ）。この暗号発生装置４１より発生された暗号キー（１）はレジスタ４２に保持されるとともに、ＣＰＵ１０の制御で再生装置６０のレジスタ６２にセットされる（図３ステップ１０ａ、図４ステップ６０ａ）。

【００５４】又、再生装置６０の暗号生成装置６１もランダムな値をもとに暗号キー（２）を発生する（図４ステップ６０ｂ）。この暗号発生装置６１より発生された暗号キー（２）はレジスタ６３に保持されるとともに、ＣＰＵ１０の制御でドライブ装置４０のレジスタ４３にセットされる（図３ステップ１０ｂ，４０ｂ）。

【００５５】ドライブ装置４０の暗号生成装置４４はレジスタ４２に貯えられた暗号キー（１）とレジスタ４３に貯えられた暗号キー（２）とを用いて暗号キー（３）を生成しレジスタ４５にセットする（図３ステップ４０ｃ）。

【００５６】又、再生装置６０の暗号生成装置６４はレジスタ６２に貯えられた暗号キー（１）とレジスタ６３に貯えられた暗号キー（２）とを用いて暗号キー（４）

を生成し、レジスタ６５にセットする（図４ステップ６０ｃ）。

【００５７】ドライブ装置４０の読出装置４６は情報記録媒体２０より複製許可情報（ＣＧＭＳ）を読出し、レジスタ４８にセットする（図３ステップ４０ｄ）。暗号化装置４９は、レジスタ４５に貯えられた暗号キー（３）を用いて、レジスタ４８にセットされた複製許可情報（ＣＧＭＳ）を暗号化処理する（図３ステップ４０ｅ。この暗号化処理された複製許可情報（ＣＧＭＳ）はＣＰＵ１０の制御で再生装置６０の復号化装置６６に渡される（図３ステップ１０ｃ）。

【００５８】復号化装置６６はレジスタ６５に貯えられた暗号キー（４）を用いて、ドライブ装置４０より受けた、暗号化処理されている複製許可情報（ＣＧＭＳ）を復号化処理し、レジスタ７１にセットする（図４ステップ６０ｄ）。

【００５９】再生装置６０内の図示しない制御装置は、レジスタ７１に貯えられた複製許可情報（ＣＧＭＳ）の内容を判断し、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“０１”で、提供情報読出し時に利用された再生装置のみに対して排他的な複製情報の再生を許可することを認識したとき、暗号化装置７０を起動する（図４ステップ６０ｅ(Yes)）。

【００６０】これにより暗号化装置７０はレジスタ６５に貯えられた暗号キー（４）を用いて、レジスタ６９に固定的に貯えられている装置固有の提供情報暗号化キー（５）を暗号化処理する（図４ステップ６０ｇ）。

【００６１】又、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“０１”でないときは、提供情報暗号化キー（５）に代わってダミーデータ（ヌル値）を生成する（図４ステップ６０ｆ）。

【００６２】ＣＰＵ１０は暗号化処理された装置固有の提供情報暗号化キー（５）又はそれに代わるダミーデータをドライブ装置４０内の復号化装置５０に転送する（図３ステップ１０ｄ）。

【００６３】復号化装置５０は再生装置６０より受けた、暗号化処理された装置固有の提供情報暗号化キー（５）を復号化してレジスタ５１にセットする。以上の処理により、暗号化及び復号化処理のための各種キー情報の設定処理が完了する。

【００６４】次に、図５及び図６に示すフローチャートを参照して、提供情報読出し時に於ける複製制御処理を説明する。ＣＰＵ１０はドライブ装置４０に対して提供情報の読出し指示を与える（図５ステップＳ１）。

【００６５】ドライブ装置４０内の図示しない制御装置は、ＣＰＵ１０より読出し指示を受けると、読出装置４６が起動する。読出装置４６は、情報記録媒体２０をドライブ制御し、情報記録媒体２０から提供情報（ＭＰＥＧ２データ）及び複製許可情報（ＣＧＭＳ）を読出す（図５ステップＳ２）。

【００６６】情報記録媒体２０から読出された複製許可情報（ＣＧＭＳ）はレジスタ４８に貯えられた後；暗号化装置４７に供給される。暗号化装置４７は、レジスタ４８に貯えられた複製許可情報（ＣＧＭＳ）の内容を判断し、ＣＧＭＳのｂ０，ｂ１が“００”であるとき、提供情報を暗号化処理せず、そのまま出力（パススルー）し、“０１”であるとき、レジスタ５１に貯えられた装置固有の提供情報暗号化キー（５）を用いて提供情報を暗号化処理し、“１１”であるとき、レジスタ４５に貯えられた暗号キー（３）を用いて提供情報を暗号化処理する（図５ステップＳ３～Ｓ７）。

【００６７】この暗号化装置４７より出力された提供情報（ＭＰＥＧ２データ）はシステムバス１０Ａを介して再生装置６０内の復号化装置６７に転送される（図５ステップＳ８）。

【００６８】再生装置６０の復号化装置６７はドライブ装置４０内の暗号化装置４７より提供情報（ＭＰＥＧ２データ）を受けると、レジスタ７１に貯えられた複製許可情報（ＣＧＭＳ）の内容を判断し、ＣＧＭＳのｂ０，ｂ１が“００”であるとき、提供情報を復号化処理せず、そのまま出力（パススルー）し、“０１”であるとき、レジスタ７２に貯えられた装置固有の提供情報暗号化キー（６）を用いて提供情報を復号化処理し、“１１”であるとき、レジスタ６５に貯えられた暗号キー（４）を用いて提供情報を復号化処理する（図５ステップＳ11～Ｓ16）。

【００６９】この復号化装置６７より出力された提供情報（ＭＰＥＧ２データ）はＭＰＥＧ２デコーダ６８によりデコード処理された後、表示コントローラ８０に送られて表示装置８１に表示出力される（図５ステップＳ17）。

【００７０】この際、ＣＰＵ１０は、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“００”であるときは、提供情報（ＭＰＥＧ２データ）を記憶装置３０に取り込むことによって、その複製情報を再生装置を特定せず任意に再生出力することができる。

【００７１】又、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“０１”であるときは、提供情報（ＭＰＥＧ２データ）を記憶装置３０に取り込むことによって、暗号化処理に供された装置固有の提供情報暗号化キー（５）キーと対をなす装置固有の提供情報暗号化キー（６）をもつ再生装置６０のみが複製情報を再生できる。

【００７２】尚、この際、複製情報をレジスタ７２に貯えられた暗号化キー（６）とともに、記憶装置３０に保存しておくことにより、その後の再生処理でレジスタ７２のキー値が書き替えられても、上記保存したキー情報を読出し、レジスタ７２に再設定することで対応する複製情報の再生が可能となる。

【００７３】又、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“１１”であるときは、提供情報（ＭＰＥＧ２デー

タ）を複製情報として記憶装置３０に取り込んでも、再生時に暗号キー（４）の値が既に変化していることから、その複製情報を復号化処理ができず、従って全ての再生装置に於いて複製情報を再生できない。

【００７４】この際、複製許可情報（ＣＧＭＳ）の内容が切り替わる度に、それに同期してレジスタ６９，７２のキー値、又はレジスタ４５，６５のキー値を新たに設定する構成とすることにより、より信頼性の高い、任意情報量単位の緻密な許可制御を可能としたコピープロテクト機構が実現できる。

【００７５】このように、情報提供側で、提供情報毎に（映画や音楽のタイトル毎に）暗号化を施すことができ、コンピュータなどで容易に情報を読み出せない構成としたことから、信頼性の高い、かつコンピュータ処理等による利用度の高い、提供情報の複製制御が確立される。

【００７６】又、コンピュータなどで読み出された情報は、読み出し時に利用された情報再生装置のみでしか複製の再生できないようにすることができることから、複製情報の正当な利用を可能にし、不当な利用を排除できる。

【００７７】上述したように本発明の実施形態によれば、大容量記録媒体等により提供される情報の受け渡しにコンピュータ装置が介在するシステムに於いても、コンピュータ装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステムが構築できる。

【００７８】尚、上記した実施形態では、情報提供媒体として、ドライブ装置を必要とするＤＶＤ、ＣＤ－ＲＯＭ等の大容量ディスクを例に採ったが、情報提供媒体が例えば通信回線を介して外部に存在するシステム構成に於いても本発明を上記実施形態と同様に適用できる。この際は、図２に示すドライブ装置４０内の読出装置４６を除く各構成要素が通信先となる外部の情報提供装置に設けて、図２に破線で示す信号路を通信路に置き換えることで容易に実現できる。

【００７９】又、上記した実施形態では、複製許可情報（ＣＧＭＳ）、及び装置固有の提供情報暗号化キー（５）をそれぞれ暗号化処理して転送しているが、必ずしも暗号化処理する必要はなく、要求される信頼性に応じて暗号化処理を省くことも可能である。

【００８０】又、上記した第２実施形態では、ドライブ装置４０及び報再生装置６０のそれぞれが、ランダムな情報をもとに一次キー情報を生成する構成としているが、これに限らず、例えば少なくともドライブ装置４０又は再生装置６０のいずれか一方が、ランダムな情報をもとに一次キー情報を生成し、当該キー情報をもとにしてドライブ装置４０及び再生装置６０がそれぞれ一時的な二次キー情報を自己生成する構成等、要は、ドライブと情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成する構成であればよい。

【００８１】又、上記した実施形態では、再生装置６０に於いて、装置固有の提供情報暗号化キー（５）と、装置固有の提供情報復号化キー（６）とをそれぞれ独立して設け、別個にレジスタ６９，７２に貯える構成としたが、これに限らず装置固有の提供情報暗号化キー（５）と復号化キー（６）とに共通のキー情報を用いてもよく、要は再生装置６０が、入力された提供情報を復号化処理するために、入力された提供情報の暗号化方式と暗号化キーの内容を把握できればよい。

【００８２】又、第２実施形態に於いては、暗号化処理に供された装置固有の提供情報暗号化キー（５）キーと対をなす装置固有の提供情報暗号化キー（６）をもつ再生装置６０のみにより複製を再生できる、一世代コピーのみを許可する複製制御機構と、全ての再生装置に於いて複製の再生を不能にした複製制御機構とを選択的に用いる構成としているが、例えばコピーフリーの複製許可モードと、全ての再生装置に於いて複製の再生を不能にする複製許可モードとを選択する構成、又は、コピーフリーの複製許可モードと、一世代コピーの複製許可モードとを選択する構成等、任意の複製許可モードの組み合わせが可能である。

【００８３】又、上記実施形態に於いては、大容量記録媒体、通信媒体等により提供される提供情報の受け渡しにコンピュータが介在するシステムを対象としているが、このシステム構成に拘らず、提供情報の受け渡しにコンピュータが直接介在しないシステム構成であっても、例えばＭＤ、ＣＤ－ＲＯＭ、ＤＶＤ等の記録媒体より提供情報を読み取るドライブ又は提供情報の送信機能をもつ通信媒体と、その読み取りデータを再生する装置との間に於いて提供情報の複製が可能な装置間のインタフェース部分に於いて、上記実施形態に示す任意の複製制御機構を適用することができる。

【００８４】又、この実施形態では、ＭＰＥＧ２により圧縮処理された映画、音楽等の提供情報を例に挙げたが、これに限らず、ＭＰＥＧＩ又はＭＰＥＧ４等により圧縮処理されたデータを含め再生対象とするシステム構成に於いても本発明を適用できる。

【００８５】

【発明の効果】以上詳記したように本発明によれば、大容量記録媒体、通信媒体等により提供される提供情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いて、コンピュータ等の複製処理が可能な装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能な複製制御方法及び複製制御装置が提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に於ける基本的なシステム構成を示すブロック図。

【図２】本発明の第２の実施形態に於けるシステム構成を示すブロック図。

【図３】本発明の第２実施形態に於ける処理手順を示すフローチャート。

【図４】本発明の第２実施形態に於ける処理手順を示すフローチャート。

【図５】本発明の第２実施形態に於ける処理手順を示すフローチャート。

【図６】本発明の第２実施形態に於ける処理手順を示すフローチャート。

【図７】本発明の実施形態に於ける情報記録媒体２０に記録されたメディア・ファイル管理情報ブロック内の複製許可情報（ＣＧＭＳ）を説明するための情報フォーマットを示す図。

【符号の説明】

１…コンピュータ装置（ＰＣ）

２…ＤＶＤ（大容量記憶媒体）

＊３…外部記憶装置

４…ＤＶＤドライブ（ドライブ装置）

６…ＭＰＥＧボード（情報再生装置）

１０…ＣＰＵ

１０Ａ…システムバス

２０…情報記録媒体

３０…記憶装置

４０…ドライブ装置

４１，４４…暗号生成装置

４２，４３，４５，４８，５１…レジスタ

４６…読出装置

４７，４９…暗号化装置

５０…復号化装置

６０…再生装置

６１，６４…暗号生成装置

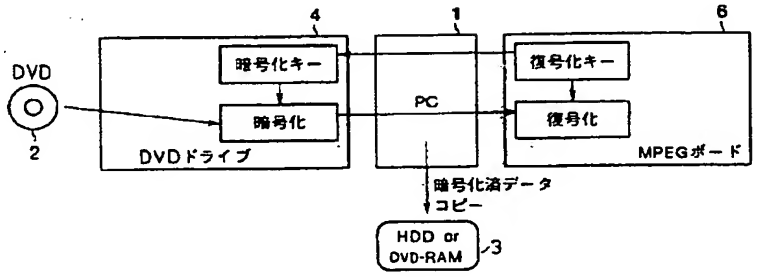
６２，６３，６５，６９、７１，７２…レジスタ

６６，６７…復号化装置

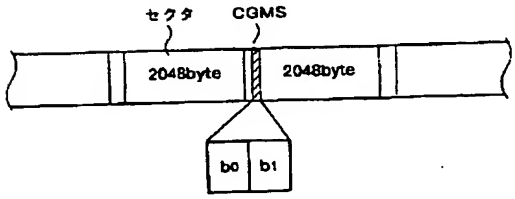
６８…ＭＰＥＧ２デコーダ

７０…暗号化装置。

【図１】



【図７】



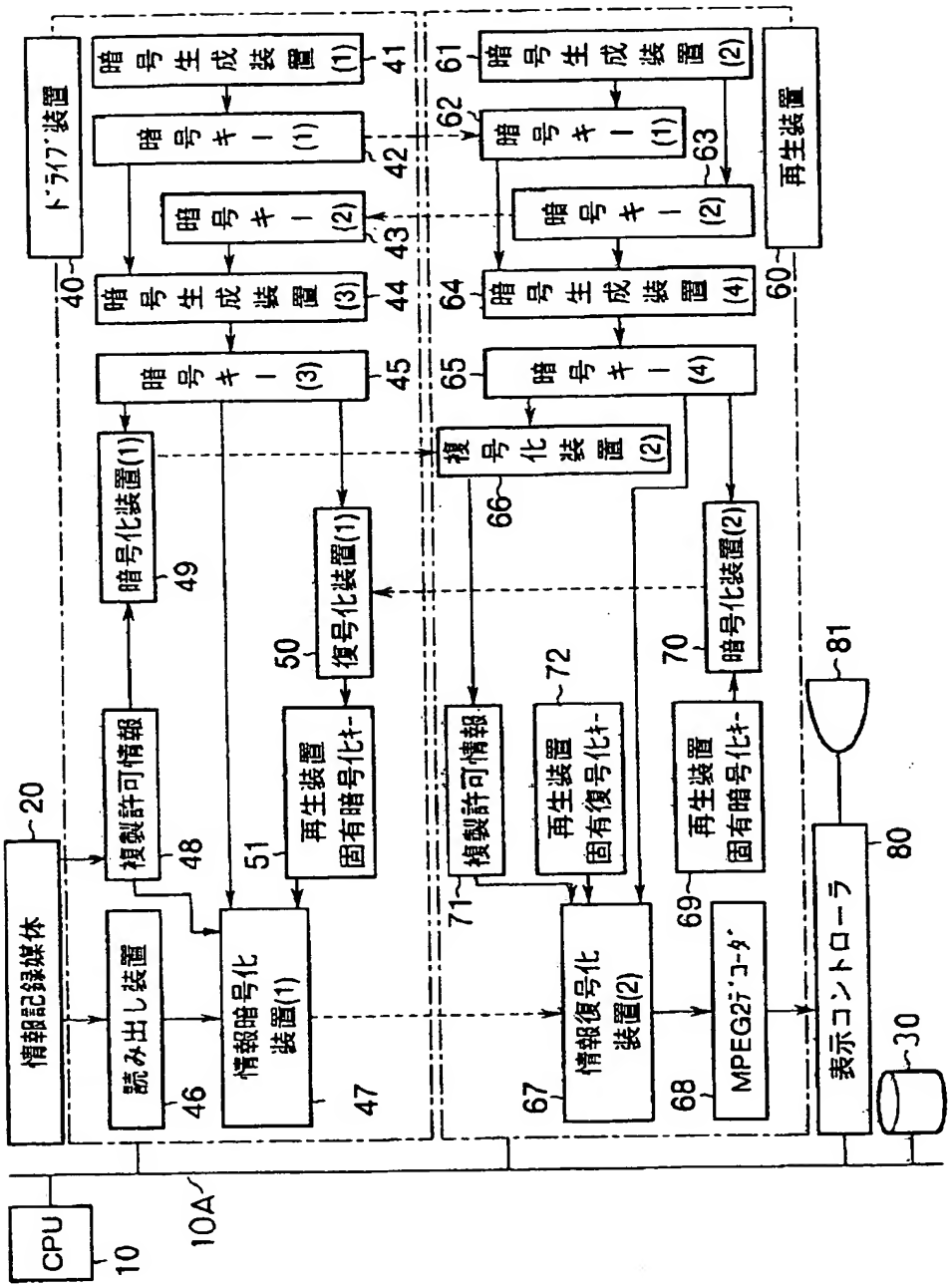
[CGMS]

b0,b1= "00" (複製の再生可)

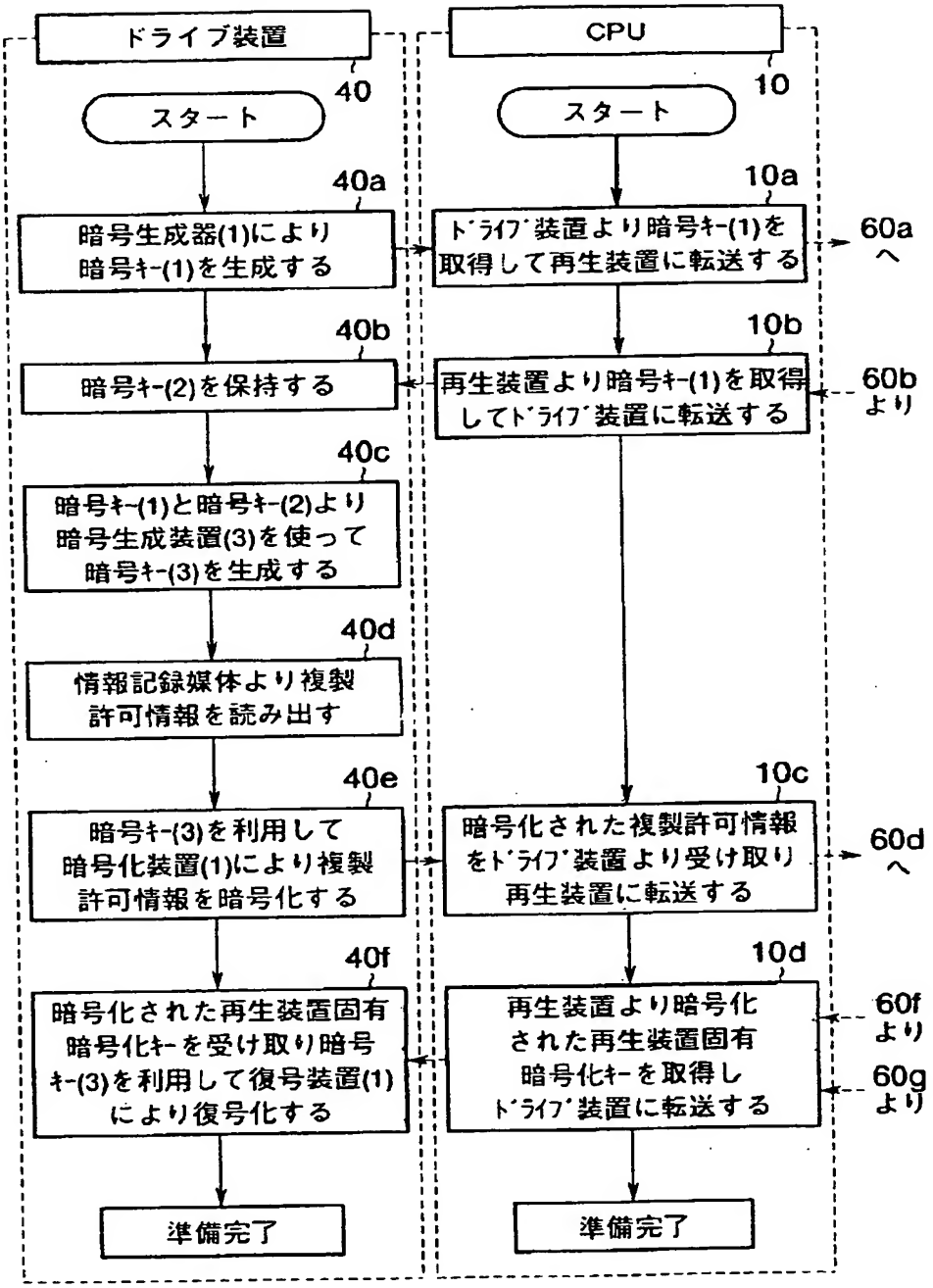
"01" (複製を作成したときに使用した装置でのみ複製の再生可)

"11" (複製の再生不可)

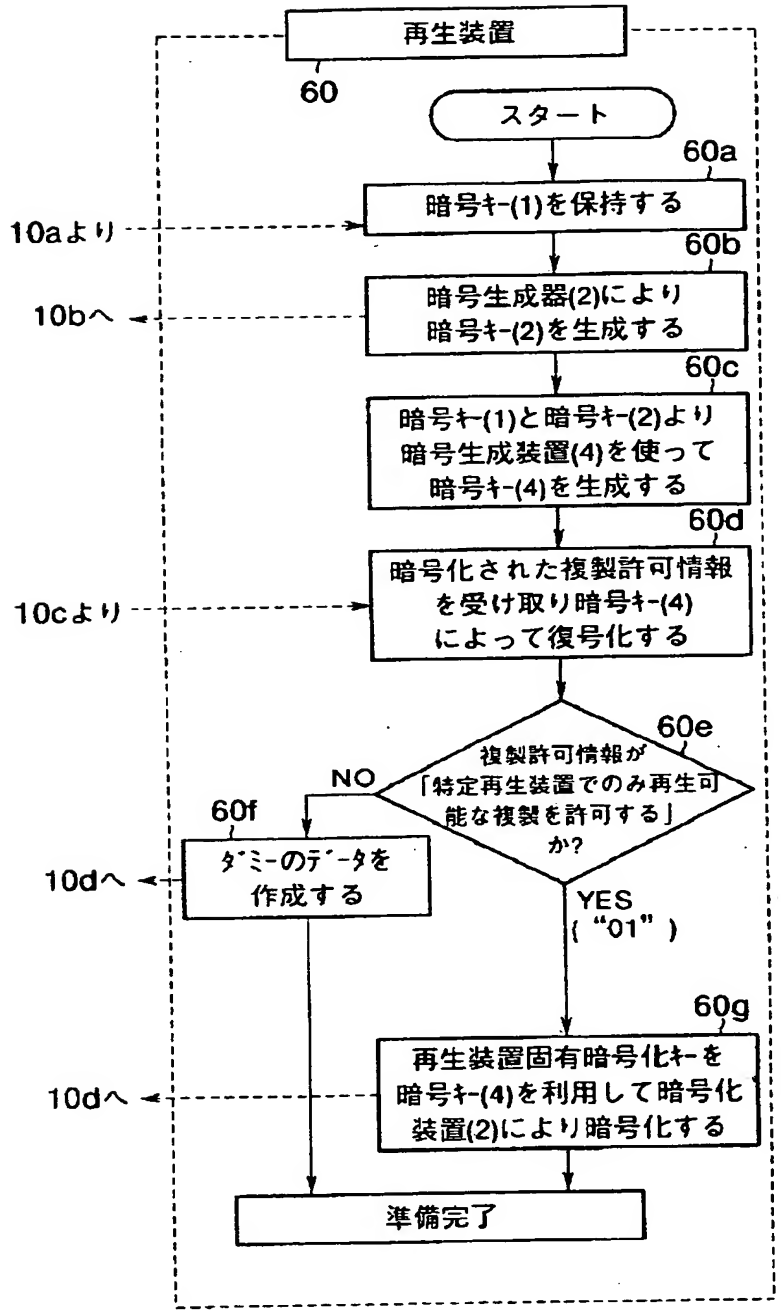
【図２】


ドライブ装置
暗号生成装置(1)
41
暗号キー(1)
42
暗号キー(2)
43
暗号生成装置(3)
44
暗号キー(3)
45
暗号化装置(1)
49
復号化装置(1)
50
再生装置固有暗号化キー
51
複製許可情報
48
読み出し装置
46
情報暗号化装置(1)
47
情報記録媒体
20
CPU
10
10A
暗号生成装置(2)
61
暗号キー(1)
62
暗号キー(2)
63
暗号生成装置(4)
64
暗号キー(4)
65
復号化装置(2)
66
暗号化装置(2)
70
再生装置固有暗号化キー
69
複製許可情報
71
再生装置固有復号化キー
72
情報復号化装置(2)
67
MPEG2デコーダ
68
表示コントローラ
80
再生装置
60
81
30

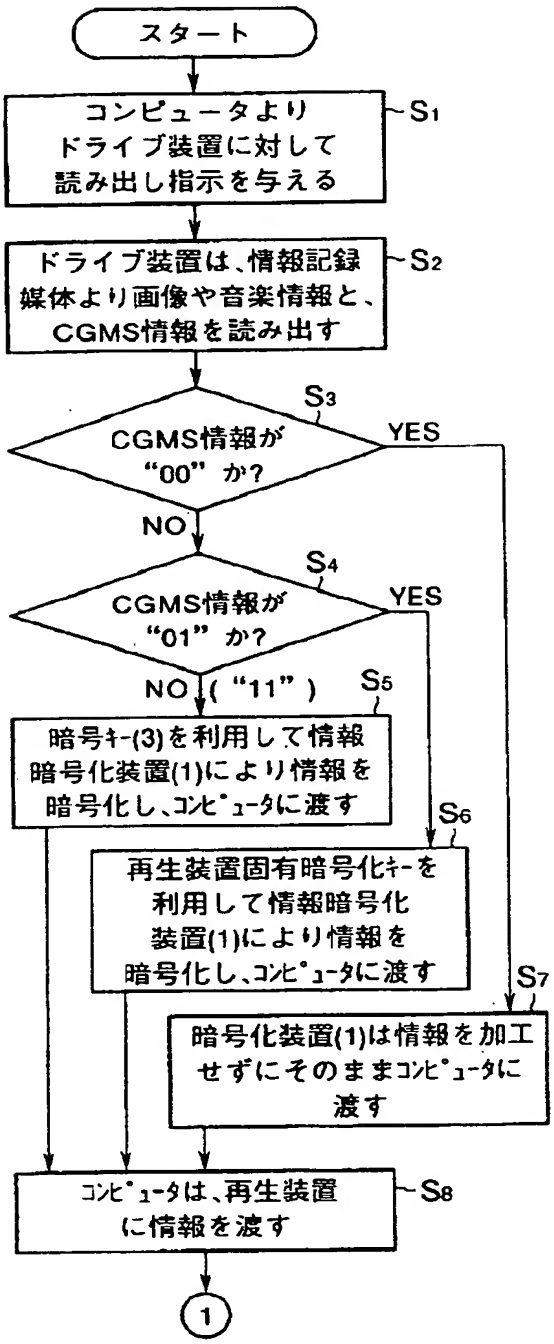
【図3】


ドライブ装置
40
スタート
40a
暗号生成器(1)により
暗号ｷｰ(1)を生成する
40b
暗号ｷｰ(2)を保持する
40c
暗号ｷｰ(1)と暗号ｷｰ(2)より
暗号生成装置(3)を使って
暗号ｷｰ(3)を生成する
40d
情報記録媒体より複製
許可情報を読み出す
40e
暗号ｷｰ(3)を利用して
暗号化装置(1)により複製
許可情報を暗号化する
40f
暗号化された再生装置固有
暗号化ｷｰを受け取り暗号
ｷｰ(3)を利用して復号装置(1)
により復号化する
準備完了
CPU
10
スタート
10a
ﾄﾞﾗｲﾌﾞ装置より暗号ｷｰ(1)を
取得して再生装置に転送する
60a
へ
10b
再生装置より暗号ｷｰ(1)を取得
してﾄﾞﾗｲﾌﾞ装置に転送する
60b
より
10c
暗号化された複製許可情報
をﾄﾞﾗｲﾌﾞ装置より受け取り
再生装置に転送する
60d
へ
10d
再生装置より暗号化
された再生装置固有
暗号化ｷｰを取得し
ﾄﾞﾗｲﾌﾞ装置に転送する
60f
より
60g
より
準備完了

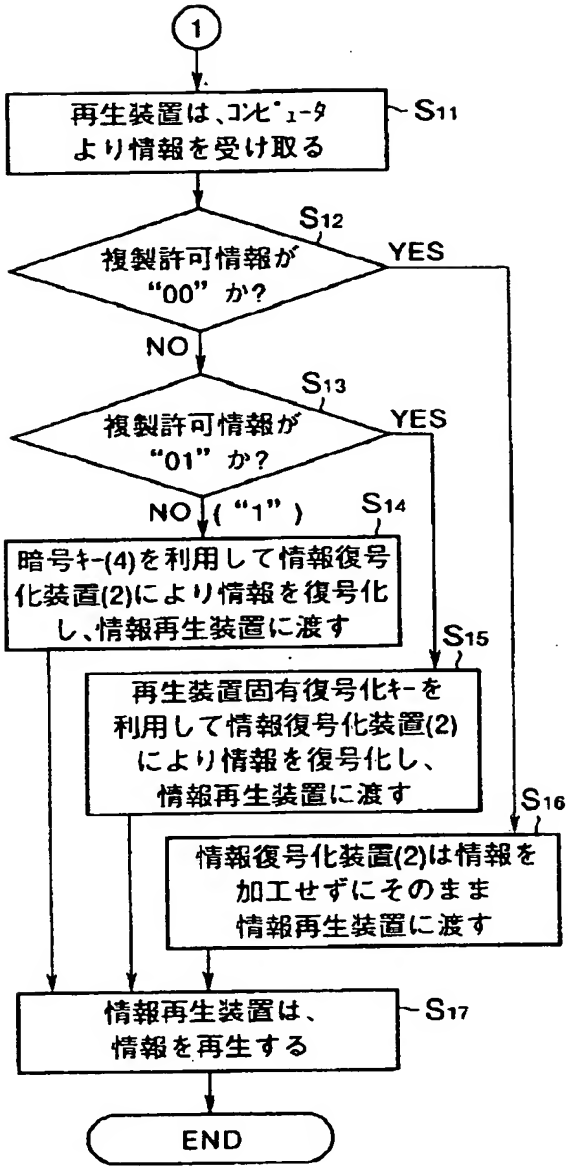
【図4】


再生装置
60
スタート
60a
暗号ｷｰ(1)を保持する
10aより
60b
暗号生成器(2)により
暗号ｷｰ(2)を生成する
10bへ
60c
暗号ｷｰ(1)と暗号ｷｰ(2)より
暗号生成装置(4)を使って
暗号ｷｰ(4)を生成する
60d
暗号化された複製許可情報
を受け取り暗号ｷｰ(4)
によって復号化する
10cより
60e
複製許可情報が
「特定再生装置でのみ再生可
能な複製を許可する」
か?
NO
60f
ﾀﾞﾐｰのﾃﾞｰﾀを
作成する
10dへ
YES
(“01”)
60g
再生装置固有暗号化ｷｰを
暗号ｷｰ(4)を利用して暗号化
装置(2)により暗号化する
10dへ
準備完了

【図５】


スタート
コンピュータより ドライブ装置に対して 読み出し指示を与える
S1
ドライブ装置は、情報記録 媒体より画像や音楽情報と、 CGMS情報を読み出す
S2
CGMS情報が “00” か?
S3
YES
NO
CGMS情報が “01” か?
S4
YES
NO (“11”)
S5
暗号ｷｰ(3)を利用して情報 暗号化装置(1)により情報を 暗号化し、ｺﾝﾋﾟｭｰﾀに渡す
S6
再生装置固有暗号化ｷｰを 利用して情報暗号化 装置(1)により情報を 暗号化し、ｺﾝﾋﾟｭｰﾀに渡す
S7
暗号化装置(1)は情報を加工 せずにそのままｺﾝﾋﾟｭｰﾀに 渡す
ｺﾝﾋﾟｭｰﾀは、再生装置 に情報を渡す
S8
1

【図６】


1
再生装置は、ｺﾝﾋﾟｭｰﾀ より情報を受け取る
S11
複製許可情報が “00” か?
S12
YES
NO
複製許可情報が “01” か?
S13
YES
NO (“1”)
S14
暗号ｷｰ(4)を利用して情報復号 化装置(2)により情報を復号化 し、情報再生装置に渡す
S15
再生装置固有復号化ｷｰを 利用して情報復号化装置(2) により情報を復号化し、 情報再生装置に渡す
S16
情報復号化装置(2)は情報を 加工せずにそのまま 情報再生装置に渡す
情報再生装置は、 情報を再生する
S17
END

【手続補正書】
【提出日】平成８年１月１０日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項１
【補正方法】変更
【補正内容】
【請求項１】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、
ドライブは、情報再生装置よりキー情報を受け、当該キー情報をもとに大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に渡し、
情報再生装置は、情報伝達手段から受けた暗号化処理された情報をドライブに発行したキー情報に関連するキー情報により復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第４区分
【発行日】平成１３年４月６日（２００１．４．６）

【公開番号】特開平９－１９０６６７
【公開日】平成９年７月２２日（１９９７．７．２２）
【年通号数】公開特許公報９－１９０７
【出願番号】特願平８－９８５
【国際特許分類第７版】
G11B 19/02 501
G06F 12/14 320
【Ｆ Ｉ】
G11B 19/02 501 Q
G06F 12/14 320 B

【手続補正書】
【提出日】平成１２年４月２５日（２０００．４．２５）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、
前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、
前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化し、前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送するステップと、
前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を複号化するステップとを具備することを特徴とする情報の複製制御方法。
【請求項２】前記生成ステップは、前記共通キーの為に少なくとも２種類の値を生成するステップを具備することを特徴とする請求項１記載の情報の複製制御方法。
【請求項３】前記暗号化ステップは、前記複製制御情報の値に従い、前記２種類の値のうちの一つを選択決定するステップを具備することを特徴とする請求項２記載の情報の複製制御方法。
【請求項４】前記生成ステップは、
前記送信装置において第１のランダム値に基づく第１のキーを生成するステップと、
前記受信装置において第２のランダム値に基づく第２のキーを生成するステップと、
前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換するステップと、
前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第１の共通キーを生成するステップとを具備することを特徴とする請求項３記載の情報の複製制御方法。
【請求項５】前記受信装置において第３のランダム値に基づく第３のキーを生成するステップと、
前記第１の共通キーを用いて、前記第３のキーを暗号化するステップと、
前記暗号化された第３のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第２の共通キーを生成するステップとを更に具備することを特徴とする請求項４記載の情報の複製制御方法。
【請求項６】前記選択決定ステップは、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第１の値を選択決定するステップを具備することを特徴とする請求項５記載の情報の複製制御方法。
【請求項７】前記選択決定ステップは、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第２の値を選択決定するステップを具備することを特徴とする請求項５記載の情報の複製制御方法。
【請求項８】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、
前記送信装置において第１のランダム値に基づく第１のキーを生成するステップと、
前記送信装置において第２のランダム値に基づく第２のキーを生成するステップと、
前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換する

ステップと、
前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、
前記送信装置と前記受信装置との間で転送される情報を保護する為の第３のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成するステップと、
前記共通キーを用いて前記第３のキーを暗号化し、第３のキーが生成されていない装置側に前記暗号化された第３のキーを前記伝達手段を介して転送するステップと、
前記暗号化された第３のキーを受信した装置側において前記共通キーを用いて前記暗号化された第３のキーを複号化するステップとを具備することを特徴とする情報の複製制御方法。
【請求項９】前記第３のキーを生成するステップは、前記受信装置において前記第３のキーを生成するステップを具備することを特徴とする請求項８記載の情報の複製制御方法。
【請求項１０】前記第３のキーを生成するステップは、前記送信装置によって読み出される複製制御情報を生成するステップを具備することを特徴とする請求項８記載の情報の複製制御方法。
【請求項１１】前記第１のキーを生成するステップは、前記受信装置からの要求に応じて前記第１のキーを生成するステップを具備することを特徴とする請求項８記載の情報の複製制御方法。
【請求項１２】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、
前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、
前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化する手段と、
前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送する手段と、
前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を複号化する手段とを具備することを特徴とする情報の複製制御装置。
【請求項１３】前記生成手段は、前記共通キーの為に少なくとも２種類の値を生成する手段を具備することを特徴とする請求項１２記載の情報の複製制御装置。
【請求項１４】前記暗号化手段は、前記複製制御情報の値に従い、前記２種類の値のうちの一つを選択決定する手段を具備することを特徴とする請求項１３記載の情報の複製制御装置。
【請求項１５】前記生成手段は、
前記送信装置において第１のランダム値に基づく第１のキーを生成する手段と、
前記受信装置において第２のランダム値に基づく第２のキーを生成する手段と、
前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換する手段と、
前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第１の共通キーを生成する手段とを具備することを特徴とする請求項１４記載の情報の複製制御装置。
【請求項１６】前記受信装置において第３のランダム値に基づく第３のキーを生成する手段と、
前記第１の共通キーを用いて、前記第３のキーを暗号化する手段と、
前記暗号化された第３のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第２の共通キーを生成する手段とを更に具備することを特徴とする請求項１５記載の情報の複製制御装置。
【請求項１７】前記選択決定手段は、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第１の値を選択決定する手段を具備することを特徴とする請求項１６記載の情報の複製制御装置。
【請求項１８】前記選択決定手段は、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第２の値を選択決定する手段を具備することを特徴とする請求項１６記載の情報の複製制御装置。
【請求項１９】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、
前記送信装置において第１のランダム値に基づく第１のキーを生成する手段と、
前記送信装置において第２のランダム値に基づく第２のキーを生成する手段と、
前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換する手段と、
前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、
前記送信装置と前記受信装置との間で転送される情報を保護する為の第３のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成する手段と、
前記共通キーを用いて前記第３のキーを暗号化し、第３のキーが生成されていない装置側に前記暗号化された第３のキーを前記伝達手段を介して転送する手段と、
前記暗号化された第３のキーを受信した装置側において前記共通キーを用いて前記暗号化された第３のキーを複号化する手段とを具備することを特徴とする情報の複製制御装置。

【請求項２０】前記第３のキーを生成する手段は、前記受信装置において前記第３のキーを生成する手段を具備することを特徴とする請求項１９記載の情報の複製制御装置。

【請求項２１】前記第３のキーを生成する手段は、前記送信装置によって読み出される複製制御情報を生成する手段を具備することを特徴とする請求項１９記載の情報の複製制御装置。

【請求項２２】前記第１のキーを生成する手段は、前記受信装置からの要求に応じて前記第１のキーを生成する手段を具備することを特徴とする請求項１９記載の情報の複製制御装置。

【請求項２３】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、

前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、

前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送するステップと、

前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を複号化するステップとを具備することを特徴とする情報の複製制御方法。

【請求項２４】前記生成ステップは、

前記送信装置において第１のランダム値に基づく第１のキーを生成するステップと、

前記受信装置において第２のランダム値に基づく第２のキーを生成するステップと、

前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換するステップと、

前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第１の共通キーを生成するステップとを具備することを特徴とする請求項２３記載の情報の複製制御方法。

【請求項２５】前記選択決定ステップは、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第１の値を選択決定するステップを具備することを特徴とする請求項２４記載の情報の複製制御方法。

【請求項２６】前記受信装置において第３のランダム値に基づく第３のキーを生成するステップと、

前記第１の共通キーを用いて、前記第３のキーを暗号化するステップと、

前記暗号化された第３のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第２の共通キーを生成するステップとを更に具備することを特徴とする請求項２４記載の情報の複製制御方法。

【請求項２７】前記選択決定ステップは、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第２の値を選択決定するステップを具備することを特徴とする請求項２６記載の情報の複製制御方法。

【請求項２８】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、

前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、

前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送する手段と、

前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を複号化する手段とを具備することを特徴とする情報の複製制御装置。

【請求項２９】前記生成手段は、

前記送信装置において第１のランダム値に基づく第１のキーを生成する手段と、

前記受信装置において第２のランダム値に基づく第２のキーを生成する手段と、

前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換する手段と、

前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第１の共通キーを生成する手段とを具備することを特徴とする請求項２８記載の情報の複製制御装置。

【請求項３０】前記選択決定手段は、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第１の値を選択決定する手段を具備することを特徴とする請求項２９記載の情報の複製制御装置。

【請求項３１】前記受信装置において第３のランダム値に基づく第３のキーを生成する手段と、

前記第１の共通キーを用いて、前記第３のキーを暗号化する手段と、

前記暗号化された第３のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第２の共通キーを生成する手段とを更に具備することを特徴とする請求項２９記載の情報の複製制御装置。

【請求項３２】前記選択決定手段は、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第２の値を選択決定する手段を具備することを特徴とする請求項３１記載の情報の複製制御装置。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】００１４
【補正方法】変更
【補正内容】
【００１４】本発明に係る情報の複製制御方法は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化し、前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送するステップと、前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を複号化するステップとを具備することを特徴とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正内容】
【００１５】また、本発明に係る情報の複製制御方法は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、前記送信装置において第１のランダム値に基づく第１のキーを生成するステップと、前記送信装置において第２のランダム値に基づく第２のキーを生成するステップと、前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換するステップと、前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、前記送信装置と前記受信装置との間で転送される情報を保護する為の第３のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成するステップと、前記共通キーを用いて前記第３のキーを暗号化し、第３のキーが生成されていない装置側に前記暗号化された第３のキーを前記伝達手段を介して転送するステップと、前記暗号化された第３のキーを受信した装置側において前記共通キーを用いて前記暗号化された第３のキーを複号化するステップとを具備することを特徴とする。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正内容】
【００１６】また、本発明に係る情報の複製制御装置は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化する手段と、前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送する手段と、前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を複号化する手段とを具備することを特徴とする。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正内容】
【００１７】また、本発明に係る情報の複製制御装置は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、前記送信装置において第１のランダム値に基づく第１のキーを生成する手段と、前記送信装置において第２のランダム値に基づく第２のキーを生成する手段と、前記送信装置と前記受信装置のそれぞれで生成した第１及び第２のキーを前記伝達手段を介して相互に交換する手段と、前記相互に交換された第１及び第２のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、前記送信装置と前記受信装置との間で転送される情報を保護する為の第３のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成する手段と、前記共通キーを用いて前記第３のキーを暗号化し、第３のキーが生成されていない装置側に前記暗号化された第３のキーを前記伝達手段を介して転送する手段と、前記暗号化された第３のキーを受信した装置側において前記共通キーを用いて前記暗号化された第３のキーを複号化する手段とを具備することを特徴とする。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正内容】
【００１８】また、本発明に係る情報の複製制御方法は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送するステップと、前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を複号化するステッ

プとを具備することを特徴とする。

【手続補正７】

【補正対象書類名】明細書

【補正対象項目名】００１９

【補正方法】変更

【補正内容】

【００１９】また、本発明に係る情報の複製制御装置は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送する手段と、前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を複号化する手段とを具備することを特徴とする。